Implementing Geospatial Visualization Techniques for Cyber Datasets

LaToya Rich, l.rich@spartans.nsu.edu

Norfolk State University

Mentor: Kyle Halliday, Halliday1@llnl.gov

Lawrence Livermore National Laboratory

ABSTRACT

The Document Exploitation (DocEx) application provides a faceted navigation interface for exploratory data analysis of structured and unstructured datasets. The aim of this project was to extend the capabilities of DocEx with geospatial visualization techniques, especially in the representation of cyber datasets. This tool plots the flow of cyber data on a map for visual analysis. This technique was implemented using Java, Google Earth, and Keyhole Markup Language.

INTRODUCTION

DocEx was created to provide a software tool for information triage. That is, to reduce the time and effort that an analyst must dedicate to finding relevant information. With that in mind, geospatial visualization of cyber datasets can enable the human mind to process and detect patterns hidden among huge volumes of information that may not be apparent in other data representations such as a bar graph or a tabular report. This comes from being able to explore both quantitative and qualitative spatial relationships within large data sets.

MATERIALS

Google Earth allows you to travel the world through a virtual globe where you are able to experience a 3D rendering of the world. KML (keyhole markup language) is a XML grammar and file format for modeling and storing geographic features such as points, lines, images, polygons, and models for display in Google Earth. A KML file is processed by Google Earth in a similar way that HTML and XML files are processed by a web browser. Thus, Google Earth acts as browsers of KML files. A KMZ file is a compressed version of a KML file. Google Earth can open KML and KMZ files if these files have the proper file name extension (.kml or .kmz)

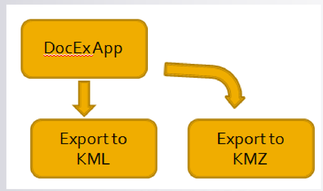

Figure 2: Demonstration of how the DocEx application will add two features using KML and KMZ

Figure 1: Snapshot of DocEx application

Figure 3: A view of what the final visualization will look like (i.e. colors, source and destination points)

METHODS

Figure 4 displays a green placemark (S) that is used for the source location and a red placemark (D) for the destination location. A line is drawn between each source and destination point representing the flow of data between two locations. The data volume is represented visually through the color of the line based on a color scale.

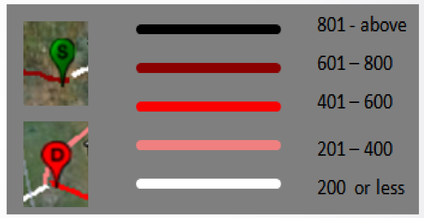

Figure 4: Displays source, destination, and path prototypes.

The snapshot below (Figure 5) shows a KML snippet dynamically generated from the Java code. The <Placemark> elements represent the endpoints, while the <LineString> elements represent the lines connecting the pairs of endpoints. The <StyleUrl> elements represent the style that each path and placemark will implement, which is shown in Figure 6.

DataFlow.java | output.kml

```
<Folder>
<Placemark>
<name>LasVegas/NV/UnitedStates</name>
<styleUrl></styleUrl>
<Point>
<coordinates>-115.17589,36.096516</coordinates>
</Point>
</Placemark>

<Placemark>
<name>"Korea,Republicof"</name
<styleUrl></styleUrl>
<Point>
<coordinates>127.5,37.0</coor
</Point>
</Placemark>

<Placemark>
<LineString>
<coordinates>
-115.17589,36.096516,0
127.5,37.0,0
</coordinates>
</LineString>
</Placemark>
```

```
<StyleMap id="msn_S0">
    <Pair>
        <key>normal</key>
        <styleUrl>#sn_S0</styleUrl>
    </Pair>
    <Pair>
        <key>highlight</key>
        <styleUrl>#sh_S</styleUrl>
    </Pair>
</StyleMap>
```

Figure 5: Shows the placemark and path generated code for the KML file. (left)

Figure 6: Show the style URL generated code for the KML file. (above)

RESULTS

The KML and KMZ export features were implemented in a Java GUI. This GUI is shown below. When the "Export to KML" button is clicked it will read data from the input file and dynamically generate a KML file. Opening the file in Google Earth shows the geospatial rendering of the network flow.

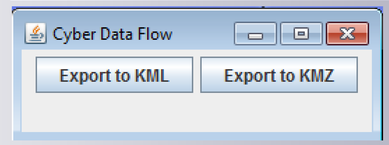

Figure 6: This shows the GUI for the two buttons.

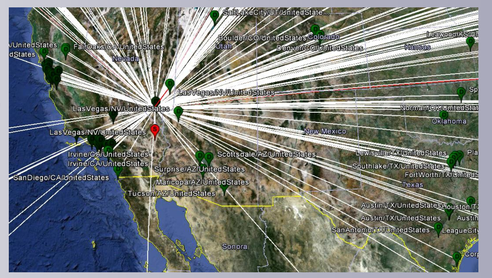

Figure 7: Zoomed in view of the results from the cyber data

FUTURE WORK

- Dynamically generating a color scale based on the input data
- Using the GUI above the "Export to KMZ" button will zip all of the information used in the KML file.
- All of the code will be embedded into the DocEx application

REFERENCES

"About KML - Google Earth Help." *Google Help*. N.p., n.d. Web. 2 Aug. 2012. <http://support.google.com/earth/bin/answer.py?hl=en&answer=148118>

"Geospatial Visualization | Where matters | Tech Trends 2012| Deloitte Consulting LLP." *Deloitte | Audit, Consulting, Financial Advisory, Risk Management and Tax Services*. N.p., n.d. Web. 1 Aug. 2012. "About KML - Google Earth Help." *Google Help*. N.p., n.d. Web. 2 Aug. 2012.<http://support.google.com/earth/bin/answer.py?hl=en&answer=148118>.

This work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344.

LLNL-POST-571533